Proskauer

Recent Class Actions Expose Data Privacy Risk in Acquisitions in Healthcare and Healthcare AI

Minding Your Business on **July 16, 2026**

The personally identifiable and health information of consumers that a company collects can be a serious consideration behind why another company would acquire it, especially given the use of data to train AI health models. This begs the question of what responsibility the acquiring and acquired companies have to protect the consumers whose data is in play.

In March of 2025, 23andMe, a company that provided direct-to-consumer genetic testing, filed for bankruptcy. Upon acquisition of the company, TTAM Research Institute said it was committed to providing customers with "choice and transparency with their data." However, due to the lack of blanket regulation in what responsibility a company has over personal health information of its customers, it can be unclear what obligations a company must comply with in a healthcare company acquisition.

General Federal Obligations under HIPAA and Section 5 of the FTC

The Health Insurance Portability and Accountability Act (HIPAA) likely first comes to mind when assessing data obligations. HIPAA mandates safeguards of health information transmitted by health care providers and insurers but not direct-to-consumers companies like 23andMe.

Second, Section 5 of the FTC Act provides for FTC enforcement of consumer privacy protections against "unfair or deceptive acts or practices in or affecting commerce." Therefore, the FTC may intervene if a company misrepresents its privacy practices or fails to implement reasonable data security measures. It did so in 2023 by filing suit against BetterHelp for selling consumers' personal information to companies like Facebook despite promising consumers safeguards over their health information. BetterHelp ended up settling for $7.8 million.

Class Actions Invoke State Data Privacy Laws, Claims of Common Law Negligence and Unjust Enrichment

The outcome of two recently-filed class actions may provide additional guidance on what companies need to do to satisfy their data privacy obligations to individuals.

One of the actions is *Kreutter v. Tempus AI, Inc.*, No. 1:26-cv-01525 (N.D. Ill.), where the most recent complaint was filed in June 2026. The plaintiffs initially provided genetic information to Ambry Genetics, the company that Tempus AI acquired. They allege that Tempus AI acquired Ambry Genetics in part to obtain its repository of patients' genetic data and use that information for commercial purposes, including training AI models and licensing data to third parties, without patients' knowledge or consent. According to the complaint, the acquisition agreement contemplated the transfer of sensitive patient data while representing that no additional patient notice or consent was required.

The plaintiffs assert claims under several state statutes:

- **Illinois Genetic Information Privacy Act (GIPA):** Prohibits the disclosure of an individual's genetic information without written consent.
- **California Confidentiality of Medical Information Act (CMIA):** Restricts the disclosure of individually identifiable medical information by healthcare providers and other covered entities without authorization.
- **Oregon Genetic Privacy Act (GPA):** Protects genetic information generally and prohibits disclosure of identifiable HIV-related testing information without authorization or another legal basis.
- **New Hampshire Data Privacy Act:** Limits the disclosure and use of genetic information without the individual's consent.
- **New York General Business Law §§ 349 and 350:** Prohibits deceptive business practices and false advertising, which plaintiffs allege were violated through misleading privacy representations regarding the collection, transfer, and commercialization of genetic data.

The complaint also includes common law claims for negligence, alleging that defendants failed to safeguard sensitive genetic information entrusted to them, and unjust enrichment, alleging that Tempus AI improperly benefited from acquiring and commercializing patients' genetic data without the consent required by law.

Under a similar set of facts, *B.W. v. Invitae Corp.* No. 2026CH05573, filed in Illinois state court under the state's GIPA, in June 2026, alleges that Invitae unlawfully disclosed its patients' (the proposed class) genetic information to LabCorp after LabCorp acquired the bankrupt testing company in 2024.

Takeaways

It can make a lot of sense to acquire a company for its data, especially to train AI health models. However, when patient or consumer data is part of the deal, especially where the data was provided upon promise to the patient or consumer that their data would be safe, companies should do their due diligence to confirm that legally effective authorization exists before data changes hands. Otherwise, they might face claims for liability under HIPAA, Section 5 of the FTC Act, related negligence and business laws, as well as state specific genetic and health privacy laws, including in Illinois, Oregon, New Hampshire and California.

Related Professionals

- **Kim Ly**
  Associate